Claims

1. A network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure network comprising a plurality of switching devices, said set of management functions comprising the recognition, operation and succession of the network configuration entity.

2. The network configuration entity of claim 1 further comprising a memory for storing an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity.

3. The network configuration entity of claim 1 wherein said set of management functions further comprise one or more rules for interaction between and among devices in the network.

4. The network configuration entity of claim 1 wherein said set of management functions further comprises device connection controls that indicate port relationships in said secure network

5. The network configuration entity of claim 4 further comprising a memory for storing a DCC list, said DCC list associated with said one or more rules for interaction between and among devices and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network.

6. The network configuration entity of claim 3 further comprising a memory for storing a DCC list, said DCC list associated with said one or more rules for interaction between and among devices and comprising definitions that logically bind each port in said secure network to one or more other ports resident in said said network.

7. The invention of claim 6 wherein said ports are identified by a unique number.

8. The invention of claim 7 wherein said unique number is a world-wide-name.

9. The network configuration entity of claim 1 wherein said set of management functions further comprises management access controls that restrict management services to a defined set of endpoints.

10. The network configuration entity of claim 9 further comprising a memory for storing an MAC list, said MAC list comprising an indication of network endpoints from which management access is acceptable.

11. The invention of claim 9 wherein said network endpoints comprise IP addresses.

12. The invention of claim 11 wherein said IP addresses are associated with access from SNMP or Telnet or HTTP or API.

13. The invention of claim 9 wherein said network endpoints comprise uniquely identified device ports.

14. The invention of claim 9 wherein said network endpoints comprise uniquely identified devices resident in said secure network.

15. The network configuration entity of claim 1 wherein said set of management functions further comprises switch connection controls for designating devices to participate in the secure network.

16. The network configuration entity of claim 15 further comprising a memory for storing an SCC list, said SCC list associated with said switch connection controls and comprising a list of devices authorized to participate in said secure network.

17. A network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, (ii) switch connection controls for designating devices to participate in the secure network, (iii) device connection controls that indicate port relationships in said secure network, and (iv) management access controls that restrict management services to a defined set of endpoints, said network configuration entity comprising;

a processor; and

a memory for storing

an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity,

an SCC list, said SCC list comprising an indication of each device allowed to participate in said secure network,

a DCC list, said DCC list comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network, and,

a MAC list, said MAC list comprising an indication of network endpoints from which management access is acceptable.

18. A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, (ii) switch connection controls for designating devices to participate in the secure network, (iii) device connection controls that indicate port relationships in said secure network, and (iv) management access controls that restrict management services to a defined set of endpoints, said Fibre Channel switching device comprising;

a processor; and

a memory for storing

an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity,

an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network,

a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network, and,

a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable.

19. A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, and (ii) switch connection controls for designating devices to participate in the secure network, said Fibre Channel switching device comprising;

a processor; and

a memory for storing

an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity, and

an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network.

20. A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, and (ii) device connection controls that indicate port relationships in said secure network, said Fibre Channel switching device comprising;

a processor; and

a memory for storing

an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity, and

a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network.

21. A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, and (ii) management access controls that restrict management services to a defined set of endpoints, said Fibre Channel switching device comprising;

a processor; and

a memory for storing

an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity, and

a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable.

22. A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) switch connection controls for designating devices to participate in the secure network, and (ii) device connection controls that indicate port relationships in said secure network, said Fibre Channel switching device comprising;

a processor; and

a memory for storing

an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network, and

a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network.

23. A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) switch connection controls for designating devices to participate in the secure network, and (ii) management access controls that restrict management services to a defined set of endpoints, said Fibre Channel switching device comprising;

a processor; and

a memory for storing

an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network, and

a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable.

24. A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) device connection controls that indicate port relationships in said secure network, and (ii) management access controls that restrict management services to a defined set of endpoints, said Fibre Channel switching device comprising;

a processor; and

a memory for storing

a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network, and,

a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable.

25. A network comprising a network configuration entity and one or more other entities, said network configuration entity having network-wide control over a defined set of management functions, said set of management functions comprising:

the recognition, operation and succession of the network configuration entity;

one or more rules for interaction between and among entities in the network;

one or more rules governing management level access to the network; and

one or more rules governing management level access to one or more entities.

26. The network of claim 25 wherein said function of recognition, operation and succession of the network configuration entity is associated with a list of network devices that are eligible to become equivalent to said network configuration entity.

27. The network of claim 25 wherein the network configuration entity has exclusive control over one or more of said management functions.

28. The network of claim 25 further comprising one or more back-up network configuration entities.

29. The network of claim 25 wherein each of said security and management functions corresponds with a data structure in a memory.

30. A method of securing a network comprising the steps of:

providing a network configuration entity having network-wide control over a defined set of management functions, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, (ii) one or more rules for interaction between and among entities in the network, (iii) one or more rules governing management level access to the network, and (iv)one or more rules governing management level access to one or more entities,

coupling said network configuration entity to one or more other devices;

placing the network configuration entity in a secure physical location; and

providing one or more back-up network configuration entities.

31. The method of claim 30 further comprising the step of placing said back-up network configuration entities in a secure physical location.

32. The method of claim 30 further comprising the step of selecting, upon a failure of the network configuration entity, a new network configuration entity from among said back-up network configuration entities.

33. The method of claim 32 wherein said selecting depends upon a pre-selected criteria.

34. The method of claim 33 wherein said pre-selected criteria is device serial number.

35. The method of claim 33 wherein said pre-selected criteria is a representation of a number uniquely identifying a device.

36. The method of claim 33 wherein said pre-selected criteria relates to the location of a device.

37. The method of claim 33 wherein said pre-selected criteria relates to the logical loading of a device.

38. The method of claim 33 wherein said pre-selected criteria relates to the functional capabilities of a device.

39. A method of securing a Fibre Channel network comprising the steps of:

defining a set of management and security functions;

designating a single entity to be responsible for implementation of said defined set of functions, wherein responsibility for implementation comprises

performing network-wide management requests, and

initiating password changes; and

limiting logical access to the network to devices designated by said single entity.

40. The method of claim 39 further comprising the steps of:

Providing a list of devices eligible to become said single entity.

41. The method of claim 40 wherein said single entity is the first listed device.

42. The method of claim 41 further comprising the step of:

upon the unavailability of said single entity, using the second listed entity as a replacement for said single entity.

43. The method of claim 41 further comprising the step of:

upon the unavailability of said second listed entity, using the third listed entity as a replacement for said single entity.

44. The method of claim 40 further comprising the steps of:

upon the unavailability of said single entity, stopping all substantive communication in the network;

re-starting substantive communication upon the availability of said single entity or a replacement for said single entity.

45. The method of claim 40 further comprising the step of:

upon the unavailability of said single entity, choosing any capable device in the network as a replacement for said single entity.

46. The method of claim 40 further comprising the step of:

upon the unavailability of said single entity, allowing no management or security function changes in the network until either (i) said single entity or a replacement for said single entity becomes available, or (ii) a predefined operator override occurs.

47. The method of claim 40 further comprising the steps of:

physically connecting a new device to the network;

first, downloading management information associated with said defined set of management and security functions from said single entity to said new device;

second, allowing said new device to logically connect to the network.

48. The method of claim 47 where in the step of allowing said new device to logically connect to the network, comprises the sub-step of distributing said management information to all other entities in the network.

49. The method of claim 47 wherein said management information comprises one or more policy sets.

50. A network switch comprising:

one or more of ports for communication information with other entities in a physical network;

a first memory for storing a list of entities eligible to be a primary network configuration entity, one of the entities on said list being the actual primary configuration entity and identifiable as such by a pre-defined rule;

a second memory for storing a network configuration policy set, said network configuration policy set comprising,

zoning information defining members of the logical zones in said physical network, and

fabric segmentation information defining management procedures to be implemented in the event that said network switch becomes a member of a segmented portion of the network.

51. The invention of claim 50 wherein said first memory and said second memory are the same.

52. The invention of claim 50 further comprising a third memory for storing MAC policies, said MAC policies defining logical channels from which a pre-defined set of security or management operations may originate.

53. The invention of claim 52 wherein said first memory, said second memory and said third memory are all the same.

54. A method of securing a network having a Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management function is controlled throughout said secure network by a network configuration entity, said method comprising the steps of :

controlling the recognition, operation and succession of the network configuration entity by designating an NCE list comprising an indication of each device in the network that may operate as said network configuration entity;

designating a unique name for each devices that may participate in the secure network;

indicating port relationships in said secure network to specifically delineate a list of unique names for ports that any given port may communicate with; and

restricting management access to a pre-defined set of access methods.